IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A system for determining an operating system of a target computer operably connected to a network, the system comprising:

first and second data packets, said first and second data packets compliant with a protocol supported by said network, said first and second data packets transmitted via said network to said target computer;

first and second operating system fingerprints comprising data bits stored in a computer-readable medium, said first and second operating system fingerprints associated with a first operating system;

a first target computer fingerprint comprising data bits stored in a computer-readable medium, said first target computer fingerprint including a representation of at least a portion of data received in response to said transmission of said first data packet;

a second target computer fingerprint comprising data bits stored in a computer-readable medium, said second target computer fingerprint including a representation of at least a portion of data received in response to said transmission of said second data packet; and

fingerprint comparison instructions executable by a computer to compare said first operating system fingerprint and said first target computer fingerprint, to compare said second operating system fingerprint and said second target computer fingerprint, and to generate a result indicative of whether said first operating system was running on said target computer;

wherein the first and second data packets each include RFC-compliant TCP packets.

2. (Original) The system as described in claim 1, wherein a first range of bits of said first data packet represents a first parameter value, and wherein said first range of bits of said second data packet represents a second parameter value different from said first parameter value.

3. (Original) The system as described in claim 2, wherein said second parameter value is derived by changing one bit in said first range of bits of said first data packet.

4. (Original) The system as described in claim 2, wherein said first and second operating system fingerprints differ.

5. (Original) The system as described in claim 4, further comprising:

a third data packet, said third data packet compliant with said protocol, said first range of bits of said third data packet representing a third parameter value different from said first and second parameter values, said third data packet transmitted via said network to said target computer;

a third operating system fingerprint comprising data bits stored in a computer-readable medium, said third operating system fingerprint associated with said first operating system, said third operating system fingerprint differing from said first and second operating system fingerprints; and

a third target computer fingerprint comprising data bits stored in a computer-readable medium, said third target computer fingerprint including a representation of at least a portion of data received in response to said transmission of said first data packet, said comparison instructions executable by a computer to compare said third operating system fingerprint and said third target computer fingerprint before generating said result.

6. (Original) The system as described in claim 5, further comprising:

fourth, fifth and sixth operating system fingerprints comprising data bits stored in a computer-readable medium, said fourth, fifth and sixth operating system fingerprints associated with a second operating system, at least one of said fourth, fifth and sixth operating system fingerprints differing from a respective one of said first, second and third operating system fingerprints;

said comparison instructions executable by a computer to compare said fourth operating system fingerprint and said first target computer fingerprint, to compare said fifth operating system fingerprint and said second target computer fingerprint, to compare

said sixth operating system fingerprint and said third target computer fingerprint, and to generate a second result indicative of whether said second operating system was running on said target computer.

7. (Original) The system as described in claim 5, wherein said protocol is TCP/IP and wherein said first range of bits corresponds to a packet field representing a maximum segment size.

8. (Original) The system as described in claim 5, wherein said first parameter value is obtained by setting no bits, said second parameter value is obtained by setting one bit, and said third parameter value is obtained by setting two bits.

9. (Original) The system as described in claim 5, wherein said first parameter value is 0, said second parameter value is 128, and said third parameter value is 128 plus a multiple of 256.

10. (Original) The system as described in claim 5, wherein said first range of bits represents at least two bytes, and wherein a value of said second parameter is obtained by setting the last bit in a byte, and a value for said third parameter is obtained by setting the last bit in a byte.

11. (Original) The system as described in claim 10, wherein said third parameter is obtained by setting adjacent bits in said first range of bits.

12. (Original) The system as described in claim 5, wherein said first, second and third data packets are transmitted in order of lowest parameter value first.

13. (Currently Amended) A system for determining an operating system of a target computer accessible via a network, the system comprising:

a plurality of data packets compliant with a protocol supported by said network, said plurality of data packets transmitted via said network to said target computer; a first

plurality of operating system fingerprints, each comprising data bits stored in a computer-readable medium, each associated with a first operating system;

a plurality of target computer fingerprints, each comprising data bits stored in a computer-readable medium, each including a representation of at least a portion of data received in response to said transmission of said plurality of data packets; and

fingerprint comparison instructions executable by a computer to compare said first plurality of said operating system fingerprint and said plurality of said target computer fingerprints, and to generate a result indicative of whether said first operating system was running on said target computer;

wherein the plurality of data packets each include RFC-compliant TCP packets.

14. (Original) The system as described in claim 13, wherein said protocol is TCP/IP and wherein each of said plurality of data packets has a different value represented in a respective packet field.

15. (Original) The system as described in claim 14, wherein said packet field is a maximum segment size field.

16. (Original) The system as described in claim 13, further comprising:

a second plurality of operating system fingerprints, each comprising data bits stored in a computer-readable medium, each associated with a second operating system, said fingerprint comparison instructions comparing said second plurality of said operating system fingerprints and said plurality of said target computer fingerprints to generate a second result indicative of whether said second operating system was running on said target computer.

17. (Currently Amended)A method for determining an operating system of a target computer accessible via a network, the method comprising the steps of:

transmitting to said target computer a plurality of data packets compliant with a protocol supported by said network;

generating a plurality of target computer fingerprints, each including at least a portion of data received via said network in response to said transmission of said plurality of data packets;

comparing said plurality of target computer fingerprints to a first set of predetermined operating system fingerprints, each of said first set of predetermined operating system fingerprints associated with a first operating system; and

generating a result indicative of whether said first operating system was running on said target computer;

wherein the plurality of data packets each include RFC-compliant TCP packets.

18. (Original) The method as described in claim 17, comprising the further steps of:

comparing said plurality of target computer fingerprints to a second set of predetermined operating system fingerprints, each of said second set of predetermined operating system fingerprints associated with a second operating system; and

generating a result indicative of whether said second operating system was running on said target computer.

19. (Original) The method as described in claim 17, wherein said protocol is TCP/IP and wherein some of said plurality of data packets have different values in the same packet field.

20. (Original) The method as described in claim 17, wherein said protocol is TCP/IP and wherein the value of the MSS option of two of said plurality of data packets is divisible by128.

21. (Original) The method as described in claim 17, wherein a first of said plurality of data packets has a maximum segment size option of 0, wherein a second of said plurality of data packets has a maximum segment size option of 128, and wherein a third of said plurality of data packets has a maximum segment size option of 384.

22. (Currently Amended) A method for identifying an operating system of a target computer via a network, the method comprising the steps of:

sending a first data packet to said target computer via said network, said first data packet complying with a protocol of said network and having a first pattern of bits in a first range of bits;

generating a first response value representing at least a portion of data received via said network in response to said sending of said first data packet;

sending a second data packet to said target computer via said network, said second data packet complying with said protocol and having a second pattern of bits in a first range of bits, said second pattern of bits different from said first pattern;

generating a second response value representing at least a portion of data received via said network in response to said sending of said second data packet;

sending a third data packet to said target computer via said network, said third data packet complying with said protocol and having a third pattern of bits in a first range of bits, said third pattern of bits different from said first or said second pattern;

generating a third response value representing at least a portion of data received via said network in response to said sending of said third data packet;

comparing said first response value to a first predetermined value associated with a first operating system;

comparing said second response value to a second predetermined value associated with said first operating system;

comparing said third response value to a third predetermined value associated with said first operating system; and

generating a value indicative of a relationship between said first operating system and said target computer;

wherein the first, second, and third data packets each include RFC-compliant TCP packets.

23. (Original) The method as described in claim 22, the method comprising the further steps of:

comparing said first response value to a fourth predetermined value associated with a second operating system;

comparing said second response value to a fifth predetermined value associated with said second operating system; and

comparing said third response value to a sixth predetermined value associated with said second operating system.

24. (Original) The method as described in claim 22, wherein no bit is set in said first pattern of bits, wherein one bit is set in said second pattern of bits, and wherein two bits are set in said third pattern of bits.

25. (Original) The method as described in claim 22, wherein the number of bytes in said second pattern of bits that have at least one bit set is greater than the number of bytes in said first pattern of bits that have at least one bit set, and wherein the number of bytes in said third pattern of bits that have at least one bit set is greater than the number of bytes in said second pattern of bits that have at least one bit set.

26. (Original) The method as described in claim 22, wherein no byte in said first pattern of bits has a least significant bit or a most significant bit that is set, wherein at least one byte in said second pattern of bits has a most significant bit that is set, and wherein at least one byte in said third pattern of bits has a least significant bit that is set.

27.-51. (Withdrawn)

52. (New) The system as described in claim 5, wherein the third data packet includes an RFC-compliant TCP packet.

53. (New) The system as described in claim 1, wherein the first data packet includes a TCP SYN packet with a maximum segment size MSS option in an options field thereof set to 0.

54. (New) The system as described in claim 1, wherein the first data packet includes a TCP SYN packet with a maximum segment size MSS option in an options field thereof set to 128.

55. (New) The system as described in claim 13, wherein at least one of the fingerprints includes the following format:

$AW_{MSS=0}$:$AW_{MSS=128}$:$AW_{MSS=384}$:TTL:DF:OS,

where:

AW refers to a TCP advertised window,

MSS refers to a TCP options maximum segment size,

TTL refers to a TCP options time to live,

DF refers to a TCP options don't fragment flag, and

OS refers to an operating system identification.

56. (New) The system as described in claim 55, wherein at least one of the fingerprints includes the following format:

$AW_{MSS=0}$:$AW_{MSS=128}$:$AW_{MSS=384}$:$OPT_{MSS=384}$:$OPT_{MSS=0}$:$OPT_{MSS=128}$:TTL:DF:FL:OS,

where:

OPT refers to TCP options bytes, and

FL refers to TCP flags.